分散式環境中基於聲譽的信任度評估機制

Reputation-based Trust Evaluation Mechanism for Decentralized Environments

許仁傑 (Jen-Chieh Hsu)
國立政治大學 資訊科學系
台北市文山區指南路二段 64 號
105753501@nccu.edu.tw

詹琨泰 (Kun-Tai Chan)
國立政治大學 資訊科學系
台北市文山區指南路二段 64 號

左瑞麟 Raylin Tso
國立政治大學 資訊科學系
台北市文山區指南路二段 64 號
raylin@cs.nccu.edu.tw

摘要

近年來區塊鏈技術及其相關應用成為熱門焦點，區塊鏈最大的特色之一即為去中心化，然而在去中心化的分散式網路中我們很難判斷對方是否可信，在傳統簽章系統中我們透過可信賴第三方擔任憑證中心為用戶簽發金鑰憑證以此建立用戶之間的信賴關係，但要在區塊鏈此種分散式網路中找到一個可信賴第三方實屬不易，並且可能會與區塊鏈的去中心化之特性背道而馳，因此本研究參考 PGP 信任網與六度分隔理論的概念建立一套可適用於分散式環境中基於聲譽的信任度評分機制，將此機制實現一個信任度評估機制購物平台，目的希望能幫助用戶更容易判斷陌生人是否可信，以降低受騙風險。

關鍵字: 區塊鏈、去中心化、PGP、智能合約、信任度

Abstract

In recent years, the blockchain technology and its relevant applications have become hot topics. The greatest feature of the blockchain is the decentralization. Nonetheless, it is difficult for us to judge whether the other person get involved in the decentralized network is credible. Furthermore, it is difficult to find a reliable third party in such a point-to-point network. Consequently, this paper utilizes the web of trust and the theoretical concepts of six degrees of separation to establish a set of reputation-based trust evaluation mechanism for decentralized environments. It is expected that achievements of the paper can facilitate people's judgment regarding the reliability of strangers and reduce the risks of being deceived.

Keywords: block chain, decentralization, PGP, smart contract, trust degree.

壹、 緒論

近年來區塊鏈成為熱門焦點，其包含去中心化、開放性、獨立性、安全性以及匿名性等特性，其中匿名性為區塊鏈上各區塊節點的身份資訊不需公開或被驗證即可以匿名的方式進行訊息傳送或交易，在現實社交環境中當我們與陌生人相遇後，也無法輕易判斷對方是否值得信賴，然而在區塊鏈此種匿名性網路中更是如此。

在常見的數位簽章系統中，使用者其公開金鑰必須透過可信賴第三方以簽發公開金鑰憑證的方式，證明使用者其公開金鑰之效力。然而要在區塊鍊此種點對點進行傳輸的分散式網路上找到一個真正的可信賴第三方實屬不易，並且可能與區塊鏈的去中心化之特性背道而馳。

以網路購物為例，近年來詐騙行為屢見不鮮，惡意商家透過不良手法及小額交易獲取優良評價，藉此騙取買家之信任。人們在購物時往往會透過朋友推薦而選擇某樣商品，藉由自己所信之人的評價對陌生的賣家產生信任關係。

而 PGP[1]即具有類似特性，其透過用戶私鑰對他人公鑰製作數位簽章的方式，將此數位簽章與其公鑰存入金鑰鏈中，並對此公鑰的所有者設定所有者信任度，當用戶接收到一封附有公鑰的陌生電子郵件且此公鑰附有金鑰鏈中某個用戶之數位簽章時，PGP 會依據金鑰鏈中用戶所設定的信任度來判斷是否該相信此陌生郵件所提供的公鑰。

因此本研究希望能透過 PGP 信任網與所有者信任度的概念建立一套能應用在智能合約的去中心化信任度評分機制，而基於區塊鏈[2]技術的智能合約[3]，其具有區塊鏈公開透明且無法變更造假之特性，因此利用在區塊鏈上智能合約也具有無法變更造假之特性，來確保信任度評估機制能確保計算的相關參數無法被變更造假，並且所有用戶皆可以驗證紀錄於智能合約中的相關交易資訊，而當用戶欲與一個目標用戶進行交易前，其可透過本研究所提出之機制計算自身與目標用戶之間的信賴度，並以此作為是否與目標用戶進行交易的參考依據。

貳、 相關研究及技術背景

一、 數位憑證

在現實生活中我們透過出示身分證、學生證與駕照等相關證明文件以表示我們的身分，而陌生人會相信我們的原因不外乎是身分證上擁有我們的照片、姓名、出生年月日、戶籍地址等資訊，其中最重要的是身分證上蓋有發行機關的鋼印以此替上面所記載的相關資訊背書，然而在虛擬網路中則必須透過公開金鑰憑證 (Public-key Certificate) 以讓他人相信我們的身分，在公開金鑰憑證中記載了使用

者名稱、所屬機關組織、使用者所擁有的公鑰等資訊以及此憑證的發行機關。

憑證中心(Certification Authority ; CA)為每個用戶簽發金鑰憑證，數位憑證的作用是證明憑證中列出的用戶合法擁有憑證中列出的公開金鑰，當任何人看見此憑證時，即可確定此憑證持有人已經由憑證中心所認證，且其憑證上所紀錄之公鑰確實由憑證持有人所擁有。

憑證中心的規模可以大至國際型組織、政府單位、企業機構等也可小至個人，其中擔任憑證中心的腳色必須擁有一個條件，那就是必須為一個可被大家所信賴的第三方。

二、 Pretty Good Privacy (PGP)

Pretty Good Privacy(PGP)是 1991 年由菲利普．齊默曼(Philip R. Zimmermann) 獨立開發的一套自由密碼軟體，其具有保密及認證等服務，可用以保護私人電子郵件與機密資料傳輸的安全性， PGP 包含許多密碼學概念如對稱式密碼、公開金鑰密碼、數位簽章、單向雜湊函數、數位憑證等，其中 PGP 的一個特色為去中心化，無法由國家政府單位或組織所控制，這使得不信任制定標準機構的人們更有意願使用 PGP 這套軟體。

在 PGP 中並不存在憑證中心為用戶簽發金鑰憑證，取而代之的是用戶對彼此的公鑰互相簽署數位簽章，並將對方公鑰與數位簽章加入自己的 PGP 金鑰鏈，其中使用者將對方的公鑰加入自己的金鑰鏈後，其可對此把公鑰設定所有者信任度，而經由簽署對方的公鑰也就代表用戶認可此把公鑰的正確性，由此建立 PGP 的信任網。

在 PGP 系統當中所有使用者皆有一組金鑰鏈，其中分為兩個部分，一個為公開金鑰鏈而另一個則是私密金鑰鏈，在公開金鑰鏈中存放了使用者認識的其他所有使用者的公開金鑰等相關資訊，而在私密金鑰鏈中則儲存使用者本身的公私鑰對及相關資訊，以下我們將根據文獻[4]中所描述的金鑰鏈結構對金鑰鏈做詳細的說明

PGP 建立信任網的方式(亦即確認公鑰正確性的方法)分為以下三種:

1.利用自己的數位簽章確認。

2.利用自己完全相信的人的數位簽章確認。

3.利用自己部分相信的人的數位簽章確認。

(一) 利用自己的數位簽章做確認

我們假設 Alice(A)與 Bob(B)為朋友，因此 A 將 B 的公鑰加入 PGP 公鑰鏈中，並以自己的私鑰對 B 的公鑰做數位簽章，某天 Bob 寄送電子郵件給 Alice，並且附有 Bob 的數位簽章，而驗證過程分成以下四個步驟 ：

(1) PGP 首先會從 A 的金鑰鏈中尋找 B 之公鑰。

(2) 若找到 B 之公鑰後檢查後方是否存在 A 之前對此公鑰簽署的數位簽章。

(3) 若存在 A 之前對此公鑰簽署的數位簽章則 PGP 從 A 的金鑰鏈中找到 A 之

公鑰，並對 A 先前對 B 所簽的數位簽章做驗證。

(4) 若數位簽章驗證無誤，則使用金鑰鏈中 B 的公鑰對電子郵件上的數位簽章做驗證，驗證成功則表示電子郵件確實是 B 所寄。

(二)利用自己完全相信的人的數位簽章確認

我們假設 Tina(T)為 Alice(A)的家人，因此在 A 的公鑰鏈中包含 T 的公鑰，並且 A 已對此公鑰附上了數位簽章，而 A 認為 T 是個可相信的人，且在 PGP 系統中可以對公鑰的所有者設定「所有者信任度」，A 對 T 之公鑰設定為「完全信任」，這表示任何公鑰若有附上 T 的數位簽章則 A 都確信此公鑰的正確性，某天 Bob(B)寄送電子郵件給 A，並且附有 T 的數位簽章，而驗證過程分成以下三個步驟：

(1) PGP 首先會從 A 的金鑰鏈中尋找 T 之公鑰，並先用 A 的公鑰對 T 之公鑰進行驗證。

(2) 若驗證無誤，則用 T 之公鑰對 B 傳來之數位簽章做驗證。

(3) 若驗證無誤，則 PGP 判斷 B 的公鑰為正確的公鑰。

(三) 利用自己部份相信的人的數位簽章確認

我們假設 David(D)與 Emma(E)為 Alice(A)的朋友，因此在 A 的公鑰鏈中包含 D 以及 E 的公鑰，並且 A 對 D 與 E 的公鑰信任度設為「部分信任」，某天 A 取得了 Julie(J)的公鑰，而此公鑰附上了 D 與 E 的數位簽章，由於有兩個部分信任的人為其公鑰背書，因此 A 的 PGP 系統承認 J 公鑰的正確性，但若 J 僅附上 D 或 E 其中一個人的數位簽章，則 PGP 就會認為此公鑰的正確係仍然不足以確認，而將 J 之公鑰判斷為無法確認的公鑰。

圖 1 表示 Alice 的 PGP 信任網，其中用粗線框住的用戶表示附有 Alice 直接簽名的正確公鑰，用細線框住的用戶表示可被判定為正確的公鑰，用虛線框住的用戶表示無法被判定為正確的公鑰。

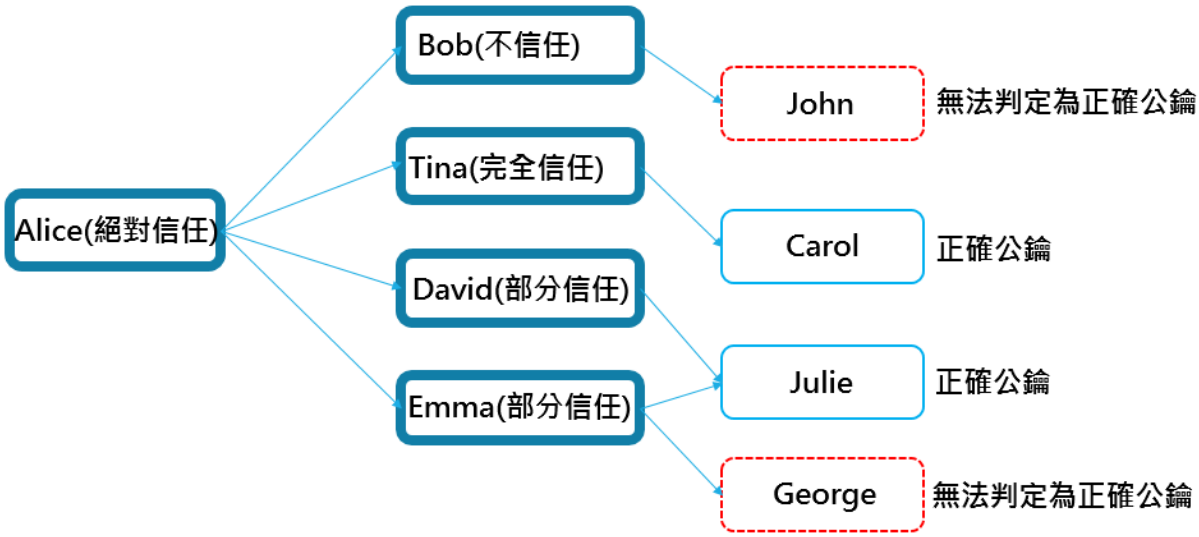

圖 1. Alice 的信任網

PGP 的概念為透過自己信賴的人而信賴陌生人，根據小世界理論[5]，兩個

陌生人最多透過 6 個人即可建立聯繫，然而 PGP 的金鑰鏈為各個用戶所獨立擁有，因此 PGP 僅能處理網路直徑為 2 的信賴關係，除非金鑰鏈中儲存的公鑰數量夠多不然很難和任何一個陌生人建立關係，在第三章中本研究參考 PGP 的概念並稍做改良，並利用智能合約實現類似公鑰鏈的紀錄表，以讓所有信任度關係可以被分享出來且不會輕易被有心人士篡改，以創造一個更完善的信任度評估機制。

三、信任度計算相關文獻

在本章第二節中我們說明了 PGP 如何建立信任網路，然而 PGP 的金鑰鏈為各個用戶所獨立擁有，因此 PGP 僅能處理網路直徑為 2 的信賴關係，除非金鑰鏈中儲存的公鑰數量夠多不然很難和任何一個陌生人建立關係，在[6]中也提到人們有時也很難判斷自己是否信任某個人，因此在與陌生人建立關係之前，若能計算出自己與陌生人之間的信任度做為參考依據，勢必能降低某種程度的風險，由此我們探討以下幾篇信任度計算的相關文獻。

在[7]中，孟等人提出於 P2P 電子商務交易環境中，兩用戶之間信任度計算的方法，計算公式如下:

$$T_{ab} = \alpha L_{ab} + (1-\alpha) R_{ab} \quad (1)$$

在公式(1)中，T_{ab}表示用戶 a 對於用戶 b 的總體信任度，L_{ab}表示直接信任度，R_{ab}表示間接信任度，α為和$1-\alpha$為直接信任度與間接信任度之權重，直接信任度公式如下:

$$L_{ab} = \frac{\sum_{i=1}^{n} V_\alpha(b,i) \cdot TA_\alpha(b,i) \cdot TT_\alpha(b,i,\Delta t)}{\sum_{i=1}^{n} TA_\alpha(b,i) \cdot TT_\alpha(b,i,\Delta t)} \quad (2)$$

其中$V_\alpha(b,i)$為用戶 a 對用戶 b 的第 i 次交易的評價，$TA_\alpha(b,i)$為該次交易金額，$TT_\alpha(b,i,\Delta t)$表示該次交易時間的衰減函數，Δt為目前時間與該次交易的時間差，由公式(2)可看出信任度會因誠信交易次數越多、交易金額越大以及交易時間差越小等因素導致信任度越高，反之則越低。間接信任度公式如下:

$$R_{ab} = \frac{\sum_{j=1}^{m} (L_{aj} \cdot L_{jb})}{m} \quad (3)$$

其中 m 為所有與用戶 b 交易過的用戶數量，L_{aj}為用戶 a 對用戶 j 的直接信任度，L_{jb}為用戶 j 對用戶 b 的直接信任度。

[7]所提出的信任度計算方法其優點為兩用戶間之信任度會因為交易次數、交易金額與交易時間差有所影響，使得計算信任度的考量得以更全面，但從公式(2)中可發現若是用戶 a 與目標用戶 b 尚未做過交易則直接信任度為 0，且在公式(3)中也僅能計算到最大網路直徑為 2 的目標用戶，因此當用戶 a 與目標用戶 b 尚未做過交易且兩用戶間網路直徑大於 2 則無法計算信任度。

在喬等人提出的[8]中，借鑒社會心理學中人與人之間的信任產生原理，提出

社交網路中基於用戶上下文的信任度計算方法，此論文所提出的信任度計算方法具有六度分隔理論的概念，因此可以解決[7]中無法計算網路直徑大於 2 的問題，而該篇研究[8]把信任度分為熟悉性產生的信任度和相似性產生的信任度，計算公式如下:

$$\mathrm{tr}(\mathrm{A},\mathrm{N}) = \mathrm{Ftr}(\mathrm{A},\mathrm{N}) + \mathrm{Str}(\mathrm{A},\mathrm{N}) \quad (4)$$

$\mathrm{tr}(\mathrm{A},\mathrm{N})$為用戶 A 對目標用戶 N 的信任度，$\mathrm{Ftr}(\mathrm{A},\mathrm{N})$為用戶 A 對目標用戶 N 由熟悉性產生的信任度，$\mathrm{Str}(\mathrm{A},\mathrm{N})$為用戶 A 對目標用戶 N 由相似性產生的信任度。

在[8]中根據六度分隔理論所說，人與人之間透過六個人即可建立聯繫，意即用戶 A 最多只需透過六層關係即可連結到目標用戶 N，由此並配合社交網路中用戶間交流溝通的次數來計算熟悉性產生的信任，公式如下:

$$\mathrm{Ftr}(\mathrm{A},\mathrm{N}) = W_N \cdot \sum_{i=1}^{n}\left[\prod_{j=1}^{m}\frac{N(S_{j-1},S_j)}{L_j}\right] \quad (5)$$

其中 i 表示用戶 A 到目標用戶 N 的 n 條路徑中的第 i 條，j 表示該路徑中的第 j 層，m 表示目標用戶所處的層數，L_j為第 j 層的所有用戶與 j-1 層中所有用戶之間的溝通次數總和，$N(S_{j-1},S_j)$為用戶S_{j-1}和S_j之間的溝通次數，S_j是該路徑上第 j 層的用戶，W_N代表目標用戶對於用戶 A 之間距離的權重。

在這先對相似性的信任度先做概略的介紹。用戶相似性所產生的信任又分為外部相似與內部相似，計算方式如下:

$$\mathrm{Str}(\mathrm{A},\mathrm{N}) = \alpha S_U(\mathrm{A},\mathrm{N}) + (1-\alpha)S_i(\mathrm{A},\mathrm{N}) \quad (6)$$

上述公式中$S_U(\mathrm{A},\mathrm{N})$表示外部相似性，其依據兩用戶間年齡與家鄉的相近性來計算，$S_i(\mathrm{A},\mathrm{N})$表示內部相似性，其依據用戶在社交網路上的興趣偏好來計算，α為調整系數。

從上述的公式裡便可得知，要計算相似性需要其他的變因才有辦法計算相似性。不論是年齡、家鄉或是興趣偏好，這些的變因要轉化成數學模型則需要再下另一番功夫。因此在本研究中僅參考熟悉性產生的信任度計算方式。

參、 基於聲譽的信任評估機制

在本章中分為兩個部分做介紹，在第一節中我們定義與介紹本機制中的相關參數設定，而在第二節中我們介紹本機制的四種評估情境以及每種情境下所對應的信任度計算公式。

一、 信任度紀錄

本機制的交易記錄數據儲存於區塊鏈上，在本機制中每一位用戶 n 擁有各自的橢圓曲線公鑰n_{pk}、私鑰n_{sk}以及三個智能合約，分別是用戶資訊合約、交易記錄表合約L_{n1}以及購買記錄表合約L_{n2}，其中用戶資訊合約存放用戶的帳號密碼與

公鑰n_{pk}。

L_{n1}為用戶 n 的交易紀錄表合約，L_{n1}紀錄買家 x 的資訊、買家 x 對用戶 n 的此次交易評價、交易金額、交易時間及買家 x 對此筆交易的數位簽章，其中交易評價 v 的區間為{1,2,3,4,5}。

表 1. 交易紀錄表$\boldsymbol{L_{n1}}$

買家資訊	交易評價	交易金額	交易時間	數位簽章
x_{info}	v	a	t	$Sign_{x_{sk}}(x_{info}, \mathrm{v}, \mathrm{a}, \mathrm{t})$

L_{n2}為用戶 n 的購買紀錄表，L_{n2}紀錄賣家 y 資訊、用戶 n 對賣家 y 此次交易的評價、交易金額、交易時間及買家 x 對此筆交易的數位簽章。

表 1. 購買紀錄表$\boldsymbol{L_{n2}}$

賣家資訊	交易評價	交易金額	交易時間	數位簽章
Y_{info}	v	a	t	$Sign_{x_{sk}}(Y_{info}, \mathrm{v}, \mathrm{a}, \mathrm{t})$

當買家對此筆交易進行評價之後，系統會將相關交易紀錄寫入買家 x 的L_{x2}與賣家 y 的L_{y1}，而在本機制中存在一個交易記錄智能合約，儲存所有用戶的交易記錄用以紀錄用戶之間的評價關係以及網路圖形，而在本機制的每個用戶都可以透過自己的公鑰對交易記錄智能合約上的交易內容進行驗證。

二、信任度評估情境與計算公式

信任根據六度分隔理論中所說，人與人之間透過六個人即可建立聯繫，但如[8]所說，在社交網路系統中依然存在孤立用戶或兩用戶無法透過其他用戶建立聯繫，在[7]所提出的信任度計算方法中，若兩用戶尚未交易過且其網路直徑大於 2 則無法計算出信任度。因此在信任度評估的過程中存在許多不同情況，故本研究提出以下四種情境：

1. 用戶 a 與目標用戶 b 曾經交易過其計算方式如公式(7)
2. 用戶 a 與目標用戶 b 無交易過但具有間接關係其計算方式如公式(8)
3. 用戶 a 與目標用戶 b 無交易過且不具有間接關係其計算方式如公式(9)
4. 目標用戶 b 尚未與任何用戶交易過其計算方式如公式(10)。

$$T_{ab} = \begin{cases} S_{ab} + O_b & (7) \\ R_{ab} + O_b & (8) \\ O_b & (9) \\ T_{initial} & (10) \end{cases}$$

在這些情境中，為了避免惡意用戶為了博取信任進一步的詐騙，因此我們將會在信任度的計算中加上所有用戶對此用戶的信任度。這樣就便可以預防曾經有詐騙前科用戶進行第二次以上的詐騙。

(一) 情境一: 兩用戶曾經交易過

在第一種情境中由於用戶 a 曾經與目標用戶 b 交易過，因此可直接透過兩用戶先前的交易紀錄來計算信任度，在公式(7)中T_{ab}代表用戶 a 對於目標用戶 b 的總體信任度，T_{ab}由直接信任度S_{ab}及全體信任度O_b組成，S_{ab}為用戶 a 對目標用戶 b 的直接信任度，S_{ab}可依據L_{a1}所記錄的相關參數做計算，S_{ab}計算公式如下：

$$S_{ab} = \frac{\sum_{i=1}^{n} v(b,i)\cdot a(b,i)\cdot t(b,i,\Delta t)}{\sum_{i=1}^{n} a(b,i)\cdot t(b,i,\Delta t)} \quad (11)$$

$v(b,i)$為用戶 a 對用戶 b 的第 i 次交易的評價，$a(b,i)$為該次交易金額，$t(b,i,\Delta t)$表示該次交易時間的衰減函數，Δt為目前時間與該次交易的時間差。O_b為依據L_{b2}中所有用戶對用戶 b 的信任度所計算出的值，公式如下:

$$O_b = \frac{\sum_{i=1}^{n} v(i)\cdot a(i)\cdot t(i,\Delta t)}{\sum_{i=1}^{n} a(i)\cdot t(i,\Delta t)} \quad (12)$$

$v(i)$為第 i 筆交易評價，$a(i)$為第 i 筆交易金額，$t(i,\Delta t)$為第 i 筆交易時間之衰減函數，Δt為目前時間與該次交易的時間差。

(二) 情境二: 兩用戶未曾經交易過但具有間接關係

第二種為用戶 a 與目標用戶 b 無交易過但具有間接關係，間接信任度關係意即兩用戶可透過其他用戶建立聯繫，在此情境中不適用於公式(7)，其原因為用戶 a 與用戶 b 不曾交易，因此L_{a1}不會紀錄關於用戶 b 的紀錄，所以在此情境下使用公式(8)，其中R_{ab}為間接信任度，其可透過交易記錄智能合約所記錄的相關參數進行計算，公式如下:

$$R_{ab} = \frac{\sum_{j=1}^{e} v(S_{j-1,}S_{j,})\cdot a(S_{j-1,}S_{j,})\cdot t(S_{j-1,}S_{j,},\Delta t)\cdot d(j)}{\sum_{j=1}^{e} a(S_{j-1,}S_{j,})\cdot t(S_{j-1,}S_{j,},\Delta t)\cdot d(j)} \quad (13)$$

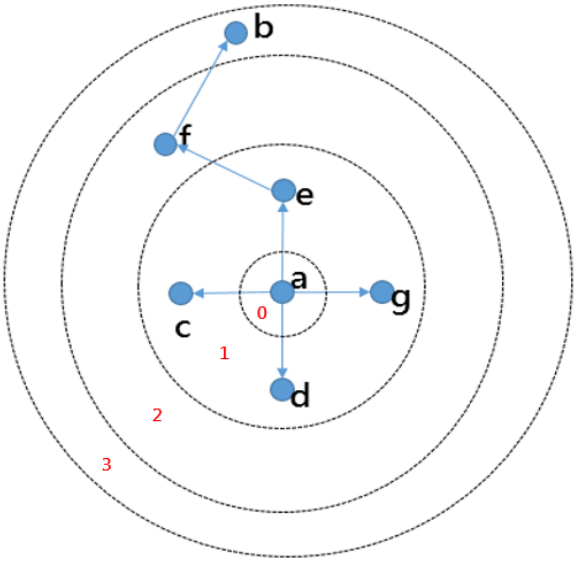

圖 2．以用戶 a 為圓心的網路關係圖形

首先我們假設用戶 a 的網路關係圖形如圖 2，在交易記錄智能合約中我們可以透過路徑演算法找出用戶 a 與目標用戶 b 之間的最短路徑P_{ab}，其中P_{ab}包含(a, e)、(e, f)與(f, b)三條路徑，意即透過 S 我們可以找出 a 對 e、e 對 f 以及 f 對 b 的交易紀錄，根據六度分隔理論，所有用戶會分布在以 a 為同心圓的 0 到 7 層同心圓當中，其中 a 處於第 0 層，在公式(13)中 j 表示P_{ab}中的第 j 層路徑，S_j表示處在第 j 層的用戶，e 為目標用戶 b 所處的層數，$v(S_{j-1}, S_j)$為S_{j-1}對S_j之交易評價，$a(S_{j-1}, S_j)$為S_{j-1}對S_j之交易金額，$t(S_{j-1}, S_j, \Delta t)$為$S_{j-1}$對$S_j$之交易時間衰減函數，而此交易時間衰減函數本研究參考[8]中的公式，而其具體定義如下:

$$t(S_{j-1}, S_j, \Delta t) = \begin{cases} 1 & \Delta t < \alpha \\ e^{\Delta t^{-1}} & \alpha \le \Delta t \le \beta \\ 0 & \Delta t > \beta \end{cases} \qquad (14)$$

α 與β為時間閾值，可依據不同情況設定其值，$d(j)$為第 j 層之距離衰減函數此函數計算出的值介於[0-1]，距離衰減函數計算公式為:

$$d(j) = \frac{7-j}{6} \qquad (15)$$

在情境二中我們透過交易記錄智能合約上所紀錄的相關資訊找尋用戶 a 與目標用戶 b 之間的最短路徑P_{ab}，然而最短路徑搜尋出的結果可能不只一條路徑。

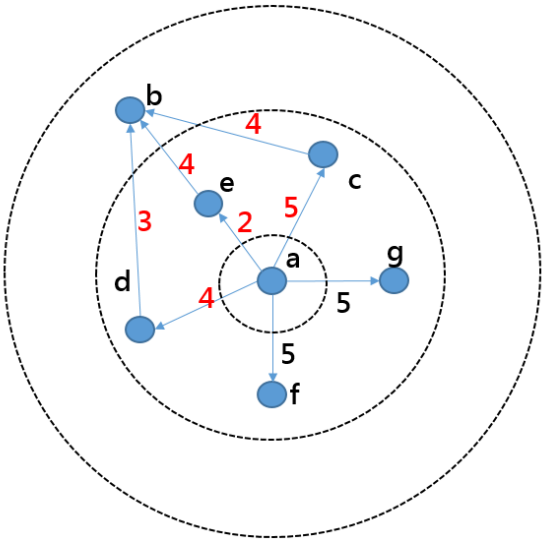

圖 3．兩用戶間具有多條最短路徑

如圖 3 所示，用戶 a 與目標用戶 b 之間其最短路徑搜尋出的結果包含{a →c → b}、{a → d→b}以及{a → e → b}等三條最短路徑，其中邊上的數字代表信任度評價權重，然而這些搜尋出的路徑可能包含用戶 a 評價較低或較不信任的用戶，因此這些不被用戶 a 所信任的鄰近用戶所提供的評價相對於被用戶 a 所信任的鄰近用戶所提出的評價較不具有參考價值，因此為了篩選出較具有參考價值的評價我們可以設定信任度閾值 T，意即若用戶 a 對相鄰的節點信任度小於 T 時，則我們不計算該條路徑，而此信任度閥值 T 可根據不同情況設定，在此我們將 T 設定為 3，由此我們可以把圖 3 簡化如下圖 4。

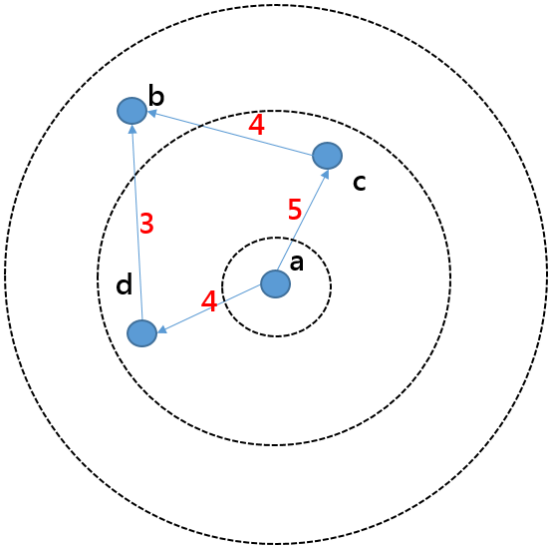

圖 4．經過信任度閾值篩選後之路徑圖形

在經過信任度閾值篩選過後，我們可利用公式(13)分別計算{a → c → b}與{a → d→ b}兩條路徑，然而此時我們會計算出利用{a → c → b}此條路徑計算出的間

接信任度R_{ab_1}以及利用{a → d→ b}此條路徑計算出的間接信任度R_{ab_2}等兩個間接信任度，因此我們必須利用權重融合R_{ab_1}與R_{ab_2}這兩條路徑，而權重來自於用戶 a 對R_{ab1}與R_{ab2}這兩條路徑上相鄰節點的信任度，其公式如下:

$$R_{ab} = \sum_{i=1}^{n} W_i R_{ab_i} \quad (16)$$

在公式(16)中 n 代表經過信任度閾值篩選後的最短路徑數量，W_i代表第 i 條最短路徑之信任權重公式如下:

$$W_i = \frac{S_i}{\sum_{i=1}^{n} S_i} \quad (17)$$

在公式(17)中S_i表示用戶 a 對第 i 條路徑上相鄰節點的直接信任度，以圖 4 的例子來說，間接信任度 $R_{ab} = W_1 R_{ab_1} + W_2 R_{ab_2}$，其中信任權重 $W_1 = \frac{5}{4+5}$，信任權重 $W_2 = \frac{4}{4+5}$ 。

(三) 情境三: 兩用戶未曾經交易且不具有間接關係

第三種情境為用戶 a 與目標用戶 b 無交易過且不具有間接關係，在此種情境下，無法計算S_{ab}與R_{ab}因此以O_b代表T_{ab}。

(四) 情境四: 目標用戶 b 尚未與任何用戶交易過

第四種情境中目標用戶 b 尚未與任何用戶交易過，因此總體信任度T_{ab}以初始信任度$T_{initial}$表示，$T_{initial}$可依據不同情況設定其值。

肆、 信任度評估機制特性之比較

一、本信任度評估機制具有之特性

在本研究中我們參考相關信任度計算文獻並將這些文獻中的優點截取並加以改良，以提出更具完善的信任度評估機制，其中本信任度評估機制具有以下幾點特性 :

(一) 可處理任意網路直徑之情況 :

網路直徑意指網路中任意兩節點之間的距離，而在本機制中我們將用戶之間的網路圖形及交易評價等相關紀錄儲存於交易記錄智能合約之中，透過路徑搜尋演算法可找出任意兩用戶之間的關係，並透過第參章中所提到的信任度計算方式即可計算出信任度。

(二) 交易金額的大小影響信任度計算結果 ：
在本研究所提出的信任度機制中，當用戶交易過後會紀錄相關交易資訊，如公式 (11) 、 (12) 以及 (13) 中我們可看出交易金額的大小會影響信任度計算出的結果，交易金額越大則此筆交易評價越具有影響力，以此避免惡意用戶透過大量小額交易換取優良評價。
(三) 交易時間影響信任度計算結果:
在公式 (14) 中，本信任度評估機制定義交易時間衰減函數，使距離目前時間越近的交易其交易評價具有較高的影響力。
(四) 具有距離權重概念:
在第參章中我們希望透過類似推薦系統的概念計算出用戶與目標用戶之間的信任度關係，然而在網路關係圖中距離自己越近的用戶代表與自己具有較直接的關係，因此如公式 (15) 所定義，我們希望距離用戶越近的其他用戶具有較大的影響力。
(五) 具有信任權重概念:
在公式 (17) 中，我們定義信任權重 W，意即用戶本身越信任的用戶其具有較高的影響力。
(六) 具有信任度閾值篩選概念:
在第參章中我們提到透過交易記錄智能合約可找到最短路徑P_{ab}，然而P_{ab}搜尋出的結果可能不僅一條路徑，在此狀況下我們透過信任度閾值的設定，篩選出信任度較高之鄰近用戶，換句話說此做法如同我們越信任的人其給予的評價越具有較高的參考價值。

二、相關文獻比較

表 3 為本信任評估機制與相關信任度計算文獻之比較表，其中 o 代表此信任度計算文獻具有表格左方所列性質之特性，x 則代表不具有此性質。本表主要是想說明在我們的機制中，我們截取這些文獻的那些特性。

表 3．信任度評估機制綜合比較表

	[6]	[7]	[8]	本機制
是否能處理任意網路直徑之情況	O	X	O	O
交易金額是否影響信任度計算結果	X	O	X	O
交易時間是否影響信任度計算結果	X	O	X	O
是否具有距離權重概念	X	X	O	O
是否具有信任權重概念	O	X	O	O
是否具有信任度閘值篩選概念	O	X	X	O

伍、結論

本研究提出在分散式環境中基於聲譽的信任度評估機制，目的希望能在沒有公正第三方的情況下依然能使買家可以容易地判斷賣家是否值得信賴，而本研究中我們也提出了四種可能情境，並且針對這四種情境分別設計出不同的信任度評

估公式以評估出最為適合的信任度分數。

另本信任度評估機制利用智能合約記錄所有用戶的交易訊息，且在本機制中所有用戶皆可驗證記錄於智能合約上的交易資訊，以確保評價的正確性，而在信任度評估公式設計方面，信任度評估的結果其影響條件包含交易金額大小、交易時間遠近、用戶之間距離的權重、信任權重以及信任度閾值等相關因素，使得計算信任度的考量得以更加全面，從而降低受騙風險。

而未來我們也將針對交易金額進行正規化的處理，以提供更準確的信任度評估分數給用戶做參考。

參考文獻

[1] Garfinkel, Simson. PGP: pretty good privacy. " O'Reilly Media, Inc.", 1995.

[2] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." 2015 IEEE Security and Privacy Workshops. IEEE, 2015.

[3] Zhang, Fan, et al. "Town crier: An authenticated data feed for smart contracts." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.

[4] WILLIAM. STALLINGS. Cryptography and Network Security: Principles and Practice. Prentice Hall, 2019.

[5] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.

[6] Y. M. Li, C. J. Chen, T. Y. Li, "A Blog System with Trust Mechanism," Proc. 18th International Conference on Information Management (ICIM 2007), Taipei, Taiwan, May, 2007.

[7] MENG, Xian-fu, Lei ZHANG, and Xu WANG. "Research on trust model of P2P electronic commerce." Application Research of Computers 8 (2009).

[8] LI, QIAO Xiu-Quan YANG Chun, and Xiao-Feng CHEN Jun-Liang. "A Trust Calculating Algorithm Based on Social Networking Service Users' Context [J]." Chinese Journal of Computers 12 (2011).